

SMART CITIES IN DARKNET ERA

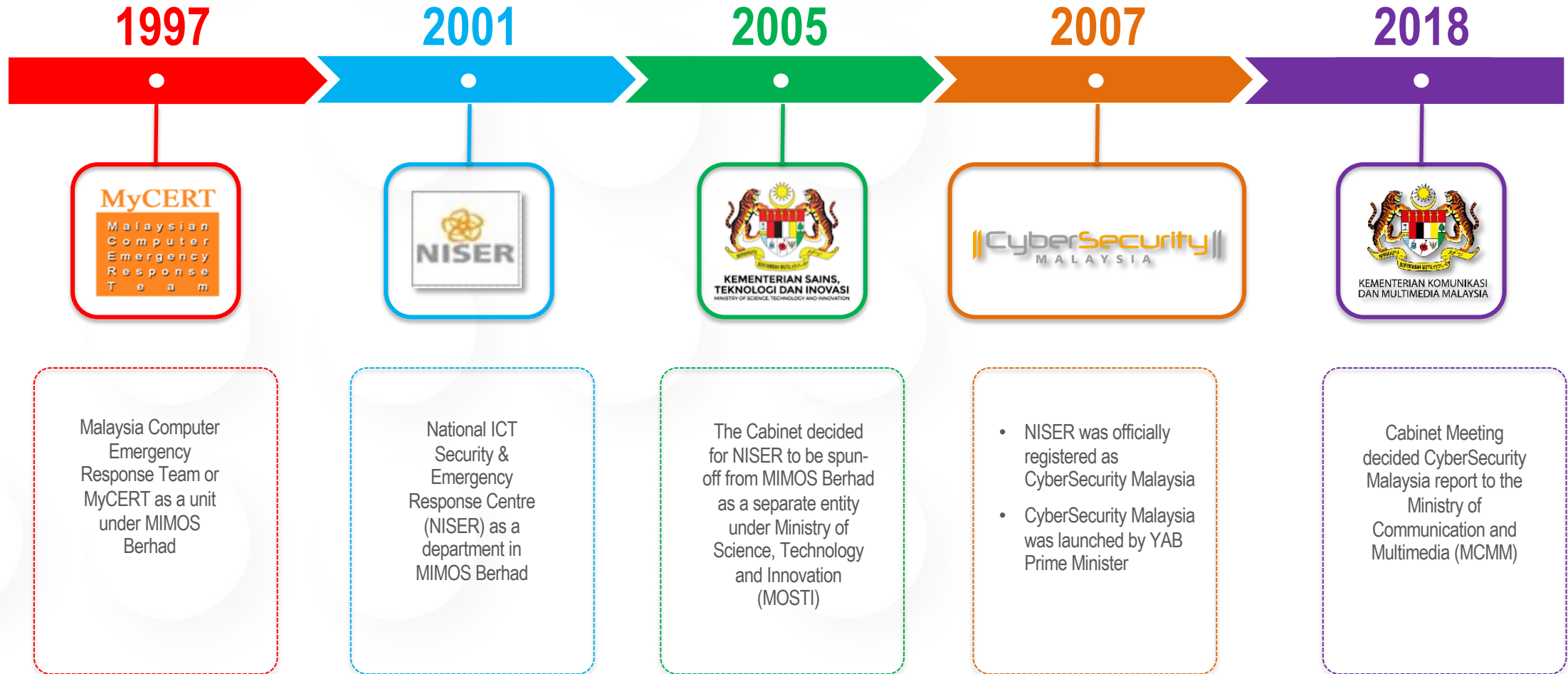
“SMART CITIES, DARKNET RESILIENCE REQUIRED ”

Nurshahira Binti Mohd,
Cyber Risk Intelligence Department



**SECURING
OUR
CYBERSPACE**

History Timelines



Visi dan Misi CyberSecurity Malaysia

VISION

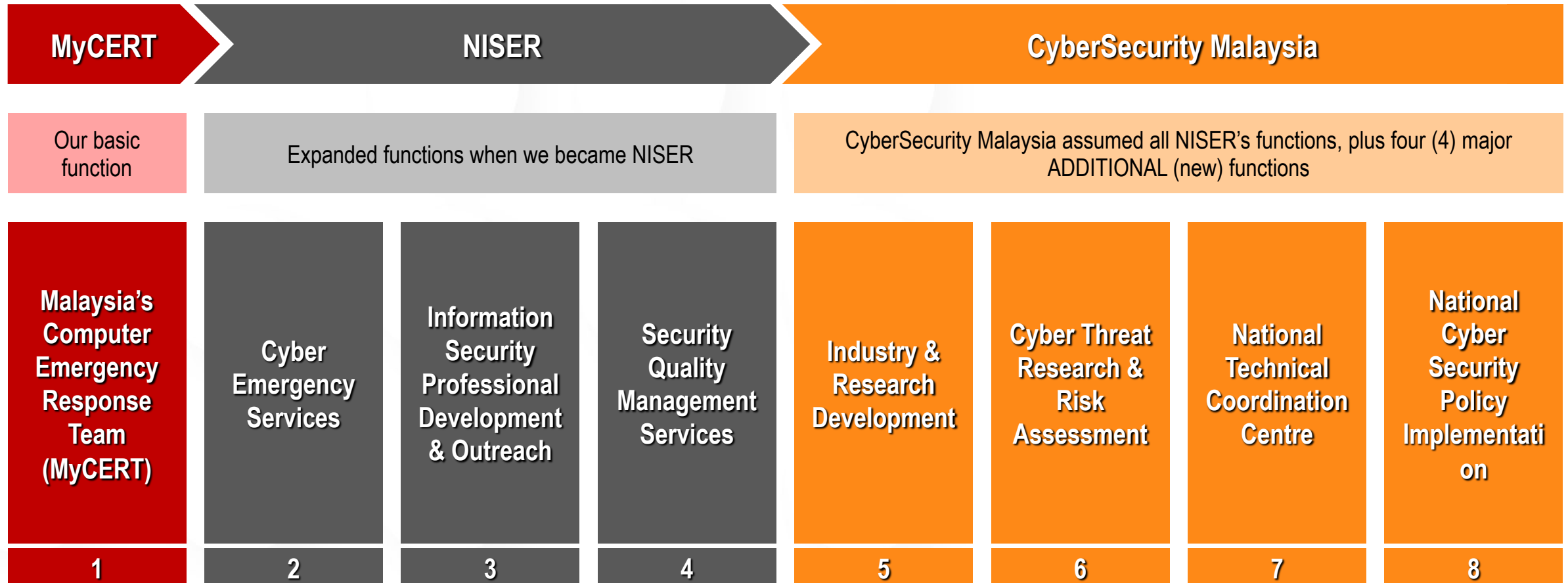
World-class cyber security specialist agency

MISSION

Leading the development of a safer and more resilient cyber ecosystem to enhance national security, economic prosperity and social harmony through

- Provision of quality and impactful services
- Frontier-expanding cyber knowledge and technical supremacy
- Continuous nurturing of talent and expertise

Our Functions



Cyber Risk Intelligence - Services



**DARKWEB
OPERATIONAL
INTELLIGENCE**



**ATTACK
SURFACE
MANAGEMENT**



**NETWORK
DEFENCE
MONITORING**

SMART CITIES IN CYBERSECURITY



A smart city is an urban environment that leverages technology to enhance the efficiency of various systems and improve the quality of life for its inhabitants. Through interconnected devices, data collection, and analysis, a smart city optimizes services like transportation, energy, healthcare, and security, fostering a more sustainable and responsive urban ecosystem.

SMART CITY & THREATS & DARKWEB



SMART CITY

Smart cities, with their interconnected systems and reliance on data, bring about numerous advantages but also introduce risks, particularly in the realm of data security:

- **Data Breaches**
- **Cyberattacks on Infrastructure**
- **IoT Device Vulnerabilities**
- **Human Error**
- **Social Engineering Attacks**

SMART CITY & THREATS & DARKWEB



THREAT



System Vulnerability



Malware



Hacker/APT/Hacktivist

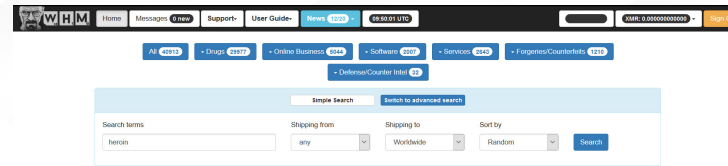


Human Error

SMART CITY & THREATS & DARKWEB



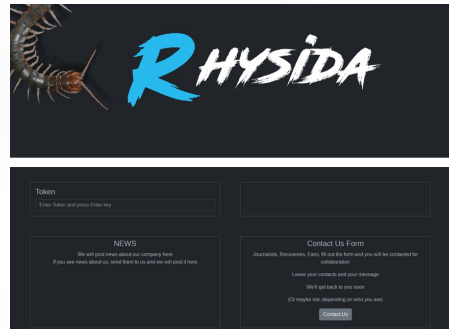
Darkweb



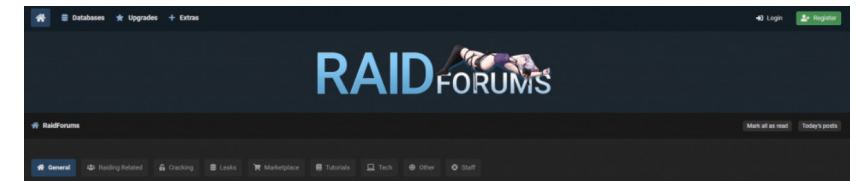
FINANCING AND FRAUD



DARKNET MARKET



RANSOMWARE



HACKING FORUM



BITCOIN SERVICE

SMART CITY & THREATS & DARKWEB

424 cameras in Iran IP:PORT,USER,PASS with snapshot links
by maraud3r - Wednesday June 14, 2023 at 12:37 PM

06-14-2023, 12:37 PM #1

424 cameras in Iran IP:PORT,USER,PASS with snapshot links

Hack any cctv camera
by kamis086 - Sunday September 24, 2023 at 01:10 PM

09-24-2023, 01:10 PM

Hidden Content

Binance verified accounts UA/EU/RU)
by juan - Saturday November 11, 2023 at 03:39 PM

11-11-2023, 03:39 PM

Selling fully verified **binance** accounts! From 30 usd. Telegram: @drorgazm

juan

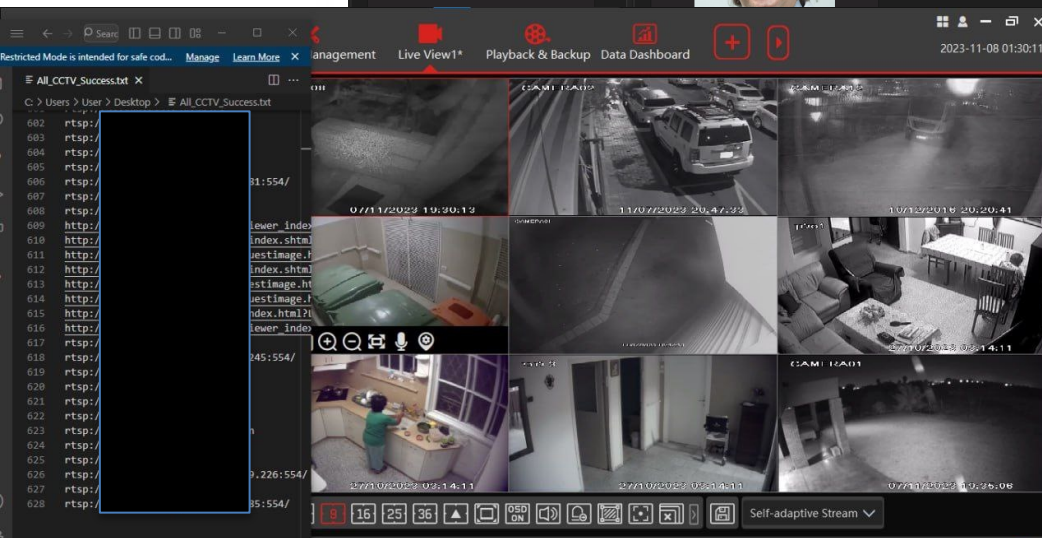
VIP User

VIP



Florida bar America state cctv hacked by Ganosecteam

[https://\[redacted\]](#)



SMART CITY & THREATS & DARKWEB



THREATS



SMART CITY

Darknet as a Destination for Stolen Smart City Data
Potential Risks Arising from Data on Darknet
Securing Smart City Data



DARKWEB

Who owns the personal data of
Malaysians?



PERSONAL DATA PROTECTION ACT 2010 (PDPA) OF ACT 709.



JABATAN
PERLINDUNGAN
DATA PERIBADI

Kementerian Komunikasi
dan Multimedia Malaysia

PRINCIPAL PARTY UNDER ACT 709

DATA USERS

Individuals or companies that process personal data in commercial transactions

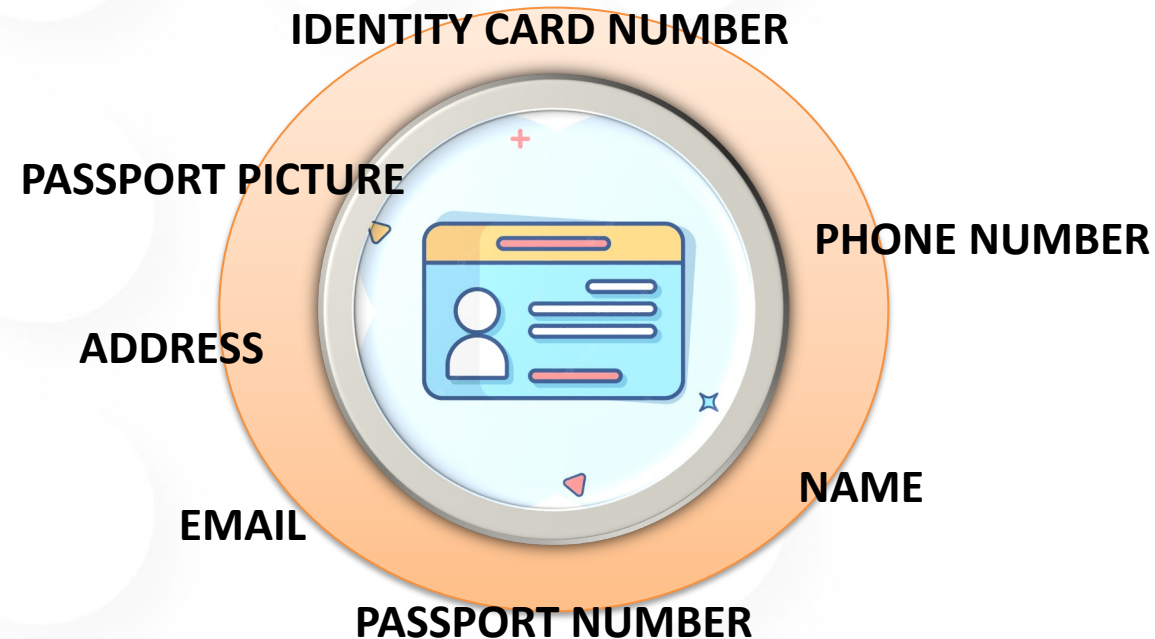
DATA PROCESSOR

Individuals or companies that process personal data on behalf of data users

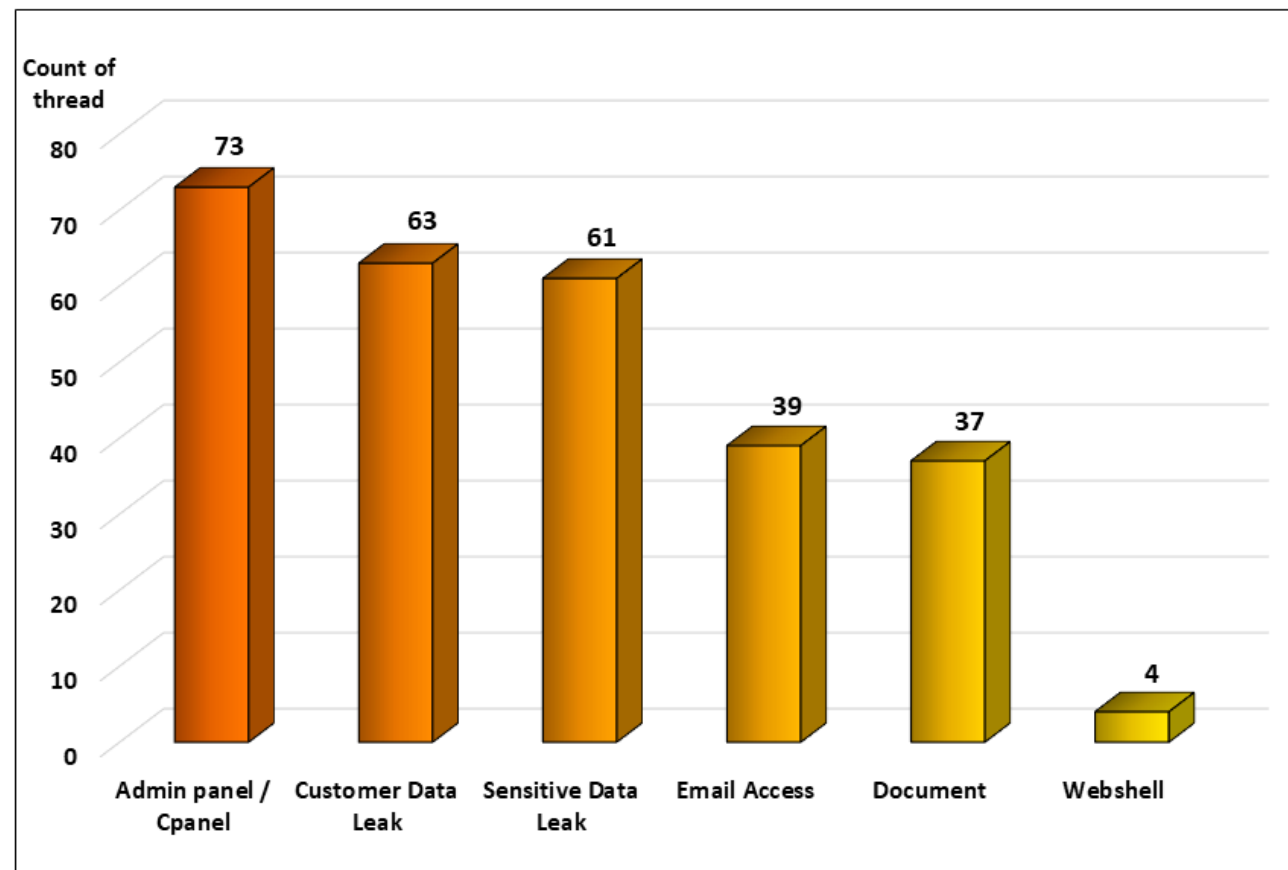
DATA SUBJECT

Owner of personal data Ex:Employees or Customers

PERSONAL IDENTIFIABLE INFORMATION



STATISTIC TYPE OF DATA LEAKAGE



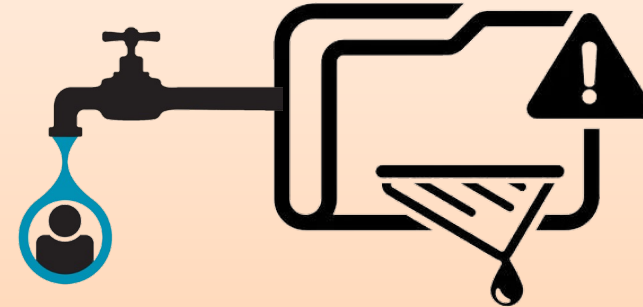
DATA BREACH VS DATA LEAK



DATA BREACH

A data breach occurs as a result of a security incident or when cybercriminals bypass security controls or launch a successful attack on systems.

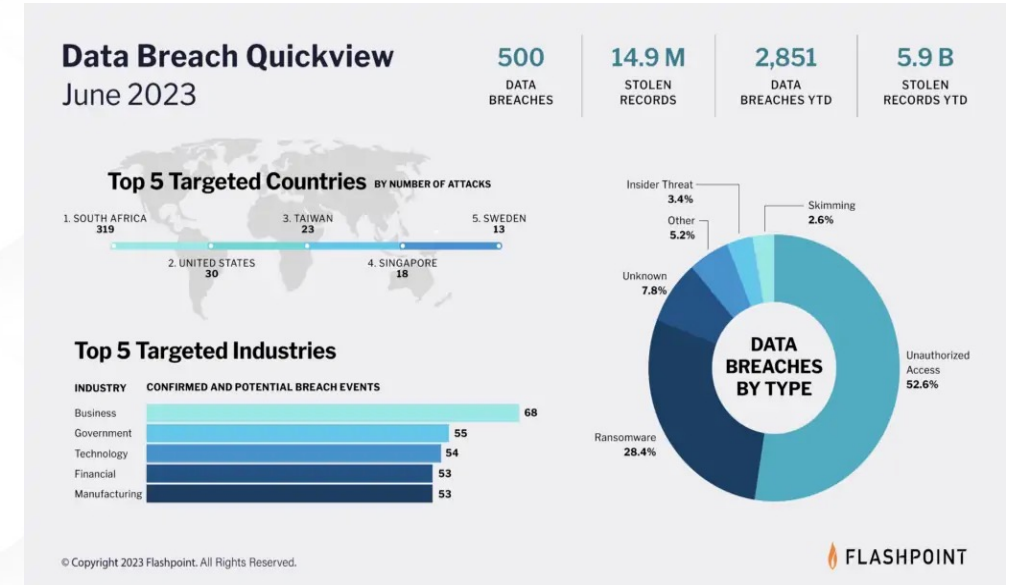
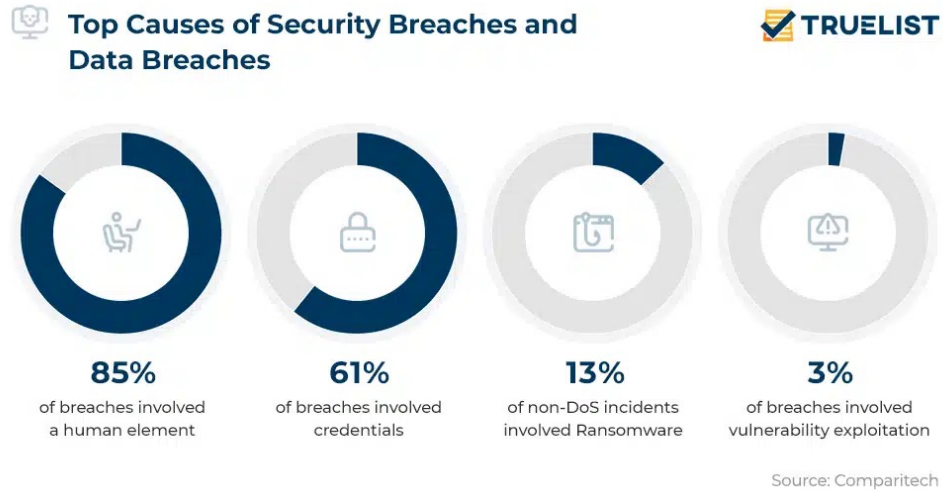
VS



DATA LEAKAGE

Data leaks happen due to missing controls and protection.

CAUSES OF DATA LEAK & BREACH

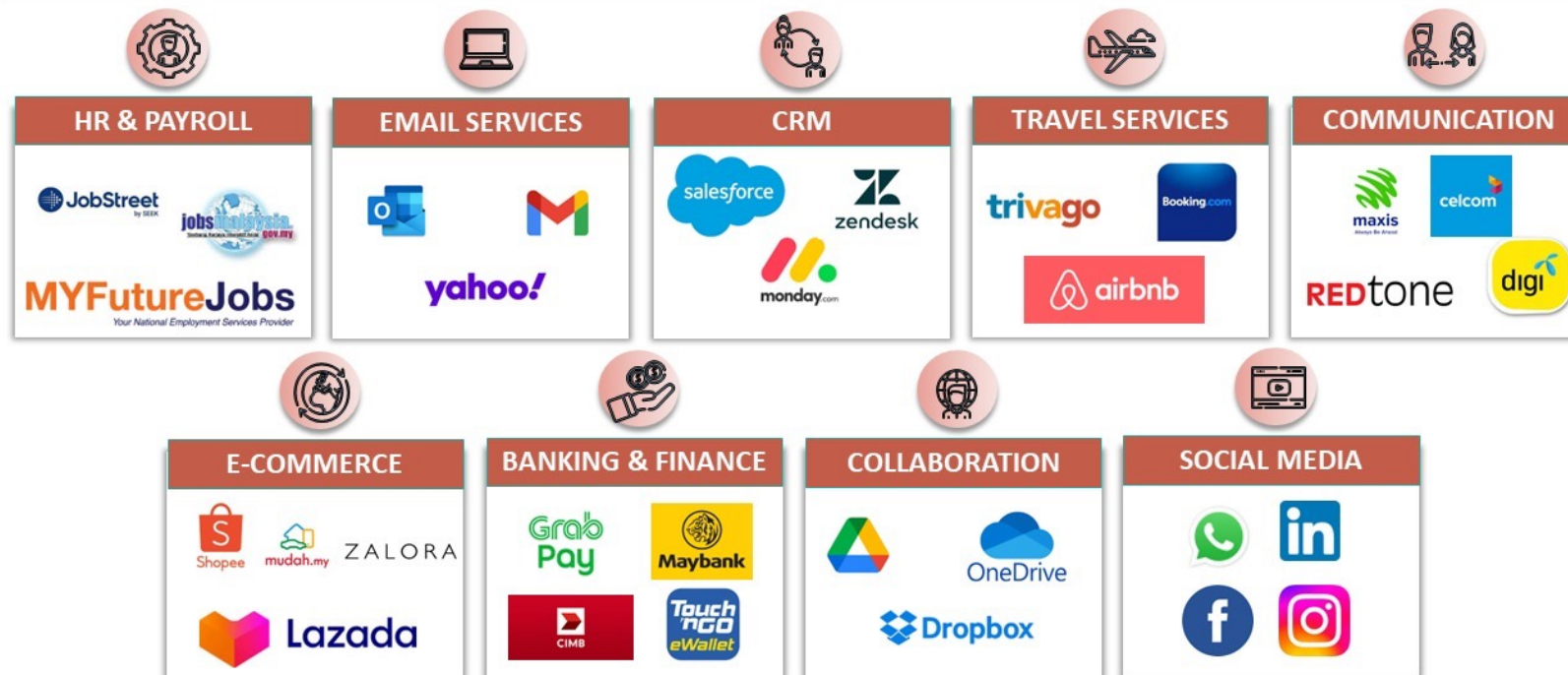


1. Insider Threat
2. Phishing Attacks
3. Malware And Ransomware
4. Weak Authentication And Authorization
5. Insecure Data Storage
6. Third-party Vulnerabilities
7. Social Engineering
8. Human Error

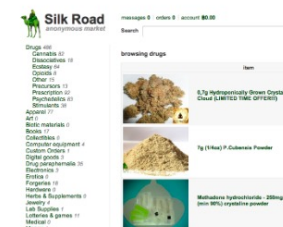
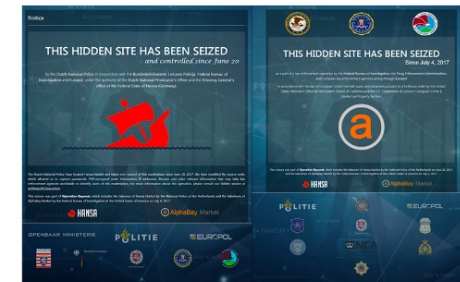
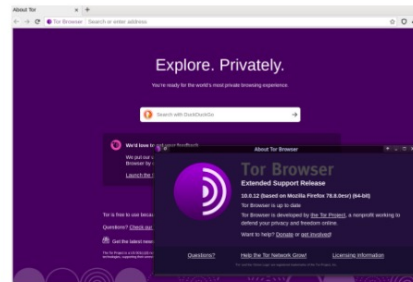
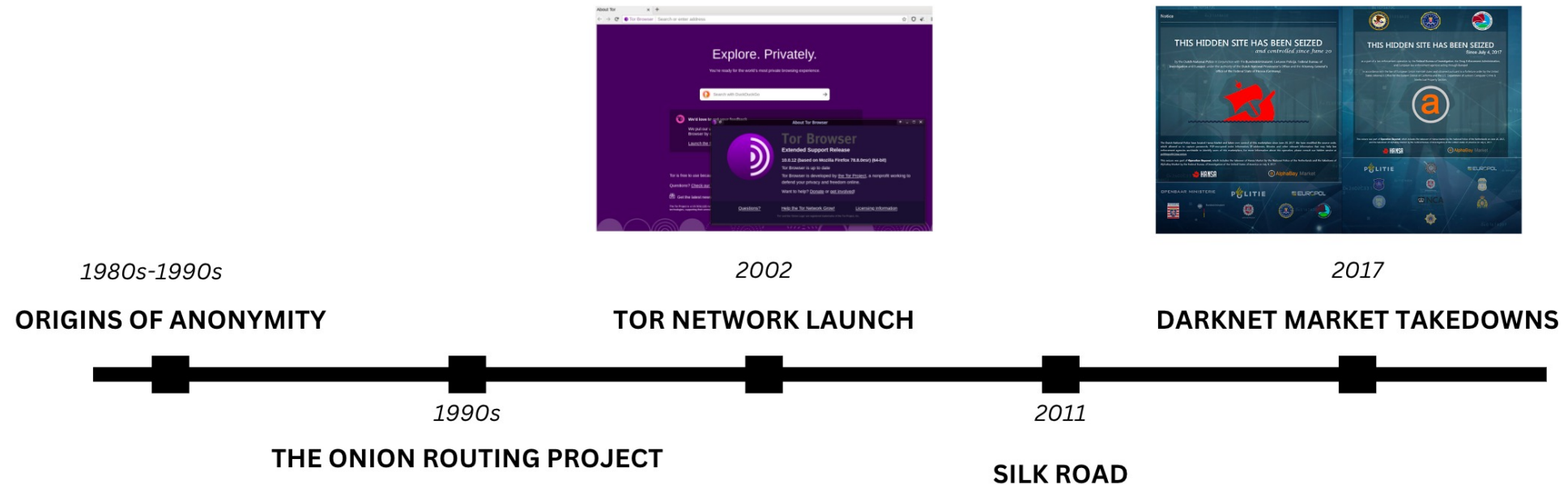
CAUSES OF DATA LEAK

THE THREAT TO ALL BUSINESS IN MALAYSIA

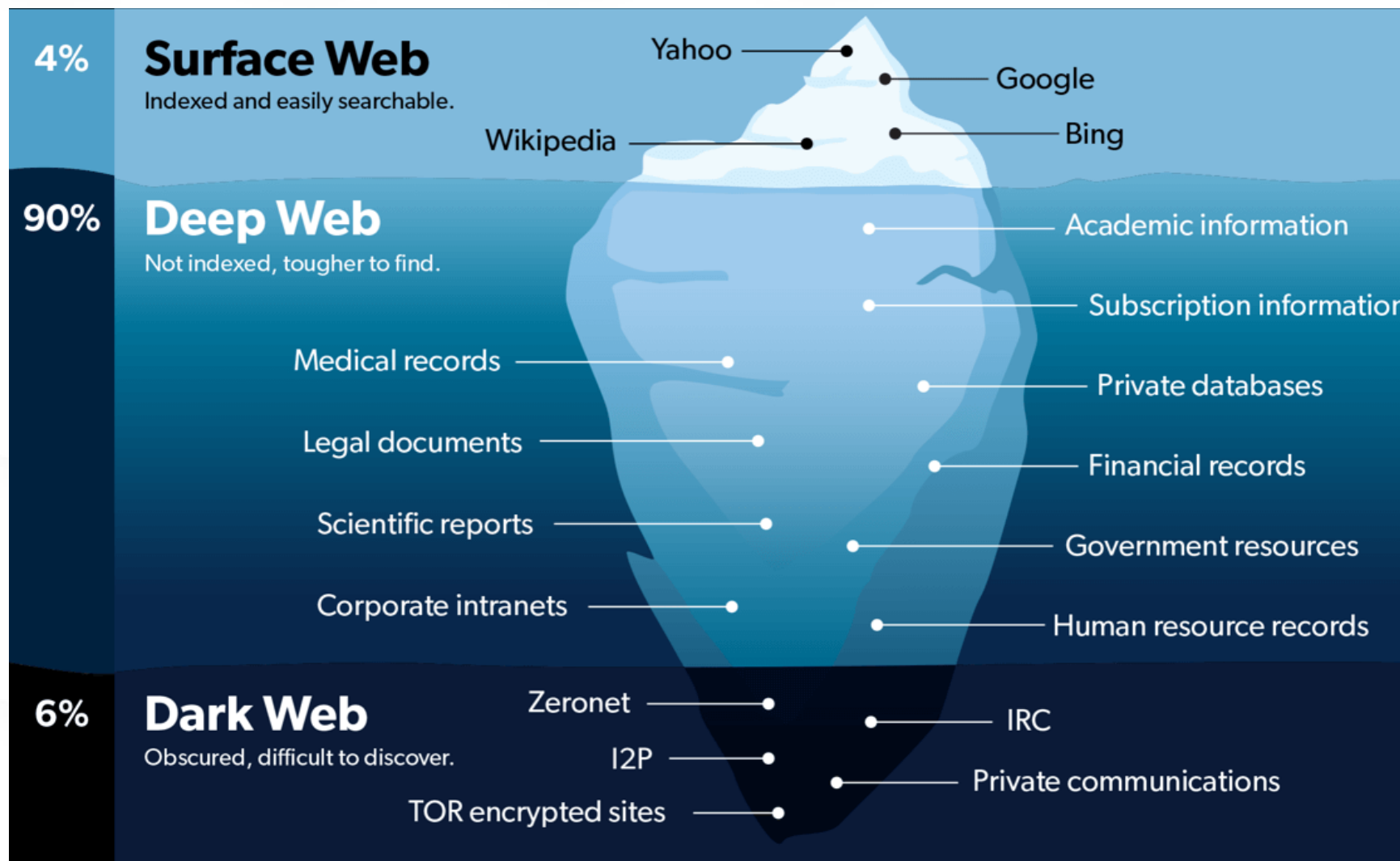
(9 ways your employees' work credentials can lead to a breach)



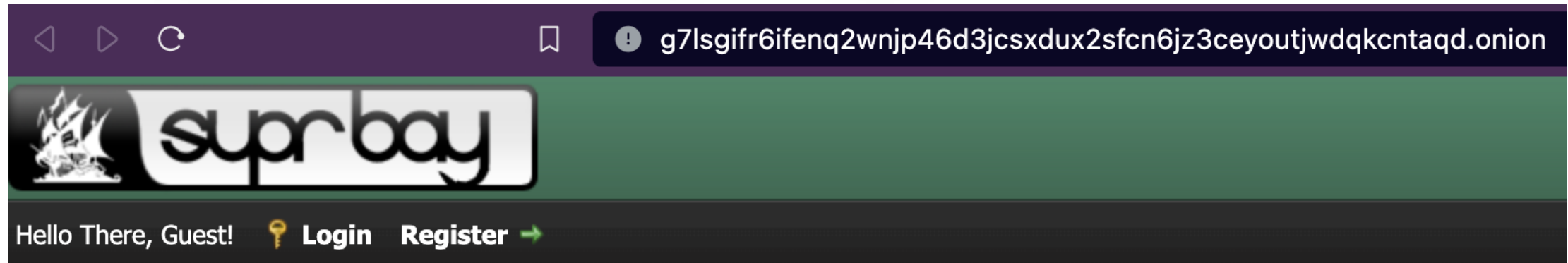
HISTORY OF DARK-WEB



WHAT IS DARK-WEB



WHAT IS DARK-WEB



DARKWEB URL CHARACTERISTIC:

1. Some of them are very long
2. Random combinations of letters and numbers
3. Ended with .onion top-level domain names.

<http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion>

<http://pqqmr3p3tppwqvvapi6fa7jowrehgd36c56l3r26qqormaqqvh6gt4jyd.onion>

<http://hydraclubbioknikokex7njhwuahc2l57lfiz7z36md2jvopda7nchid.onion>

<http://tmglstds6usxqsgghympkjbddume3olbvpqdrpxvcplhd4z7bxucdid.onion>

<http://mlyusr6htlxsyc7t2f5z53wdxh3win7q3qpxcrbam6jf3dmua7tnzuyd.onion>

<http://asap2u4pvplnkz17ecle45wajoinftja44wvovl3jrvhangeyq67ziid.onion>

<http://darkzzx4avcsuofgfez5zq75cqc4mprjvfqywo45dfcaxrwqg6qrlfid.onion>

<http://rrlm2f22lpqgfhyydqkxxzv6snw55qvc2krjt2q557l7z4te7fsvhbid.onion>

ACTIVITY IN DARK-WEB



RANSOMWARE

FINANCING AND FRAUD



DARKNET MARKET



HACKING FORUM



ILLEGAL PORNOGRAPHY

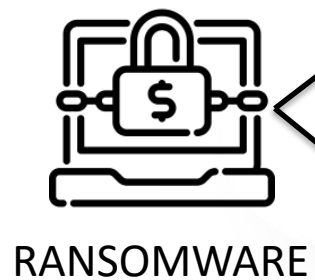


SOCIAL MEDIA



BITCOIN SERVICE

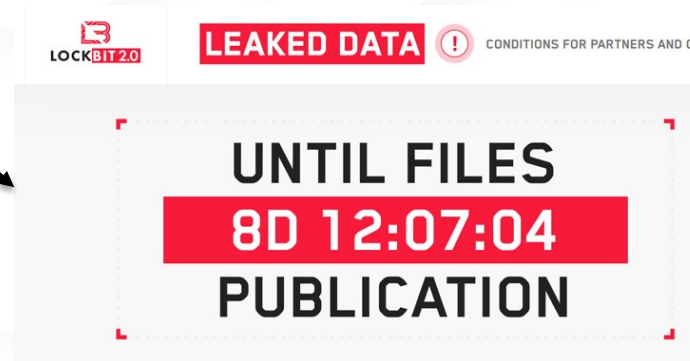
RANSOMWARE



METHOD



MOTIVATION



RANSOMWARE INCIDENT



LEAKED DATA

[TWITTER](#)
[PRESS ABOUT US](#)
[HOW TO BUY BITCOIN](#)
[AFFILIATE RULES](#)
[CONTACT US](#)
[MIRRORS](#)

UNTIL FILES 2D22H13M10S PUBLICATION

Deadline: 15 May, 2023 21:09:46 UTC



bankbsi.co.id


On May 8, we attacked Bank Syariah Indonesia, completely stopping all of its services. The management of the bank could not think of anything better than to brazenly lie to their customers and partners, reporting some kind of "technical work" being carried out at the bank.

We also want to inform you that in addition to the paralysis of the bank, we stole about 1.5 terabytes of private data.

The stolen data includes:


- 1) 9 databases containing personal information of more than 15 million customers, employees (phone numbers, addresses, names, document information, account amounts, card numbers, transactions and much more)
- 2) financial documents
- 3) legal documents

Chat: *****6B2E47



You will find out about this after all the stolen data is published, in case you do not want to pay for a quality pentest of your corporate network.
13.05.2023 13:29:28 UTC

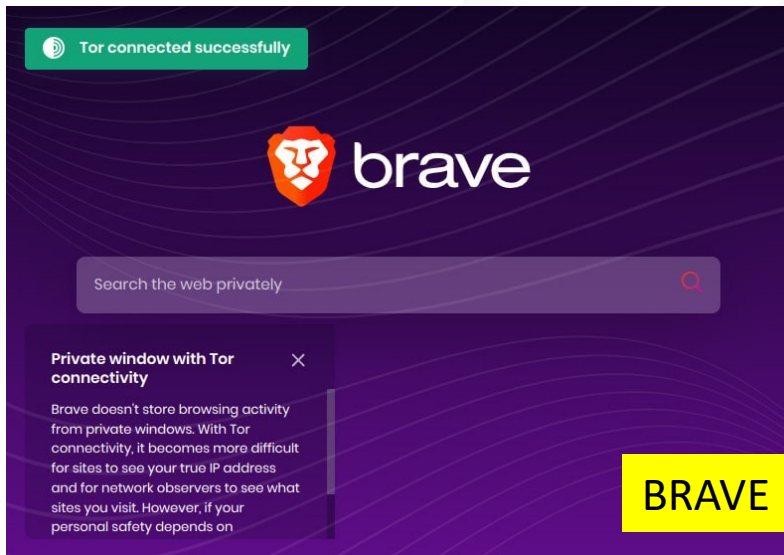
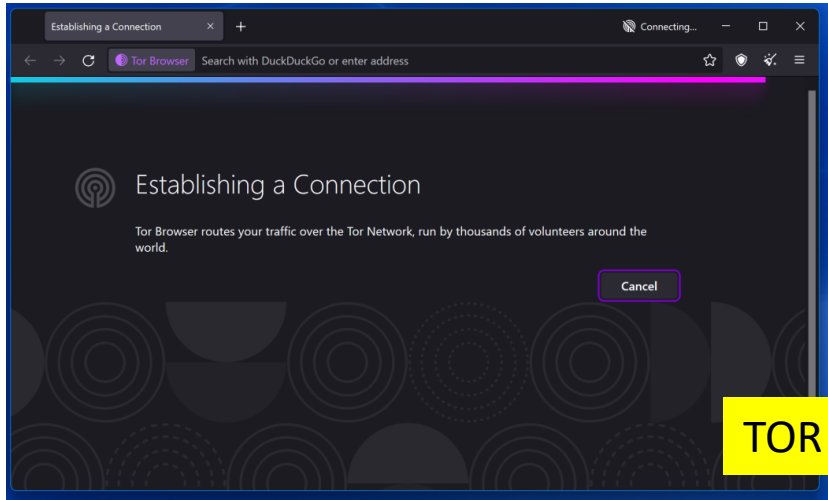
ok, can I buy for 100,000 USD? you like?
13.05.2023 14:27:05 UTC



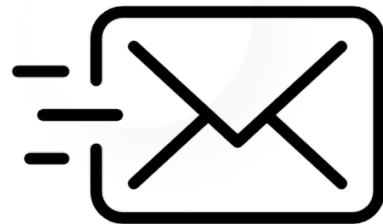
20 000 000 \$
13.05.2023 15:31:53 UTC

why is it so big, at least give us 1 sample username and password you stole we will take it at 10,000,000 dollars
13.05.2023 15:55:53 UTC

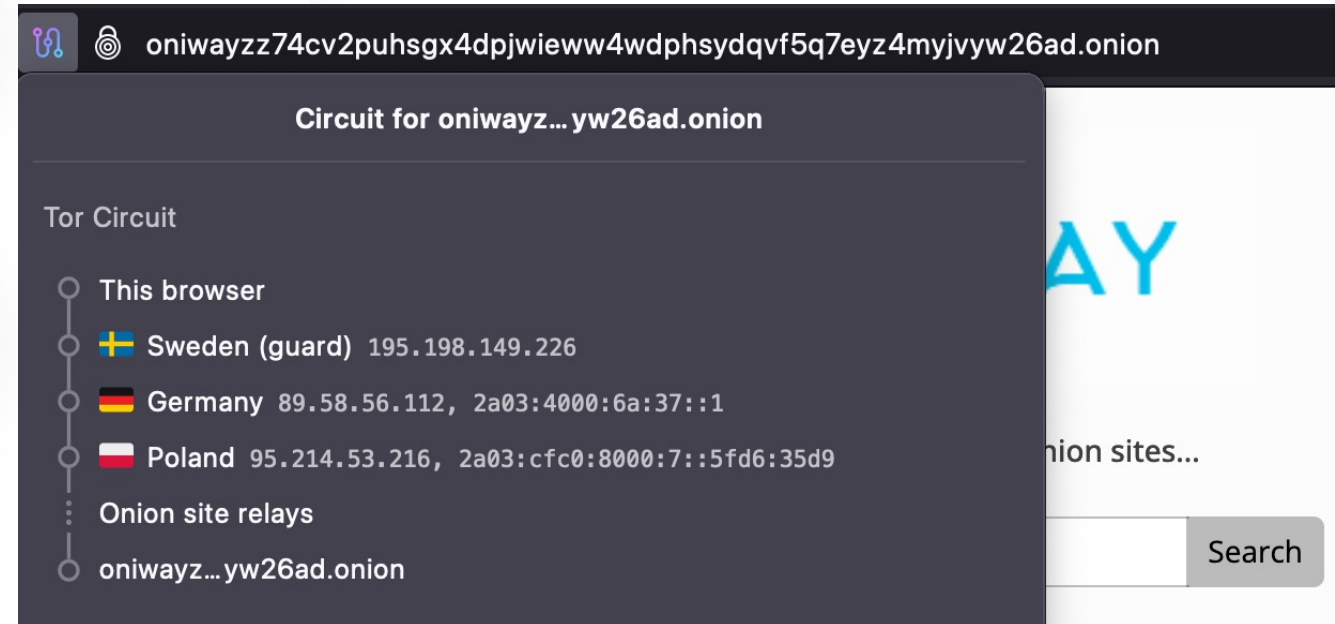
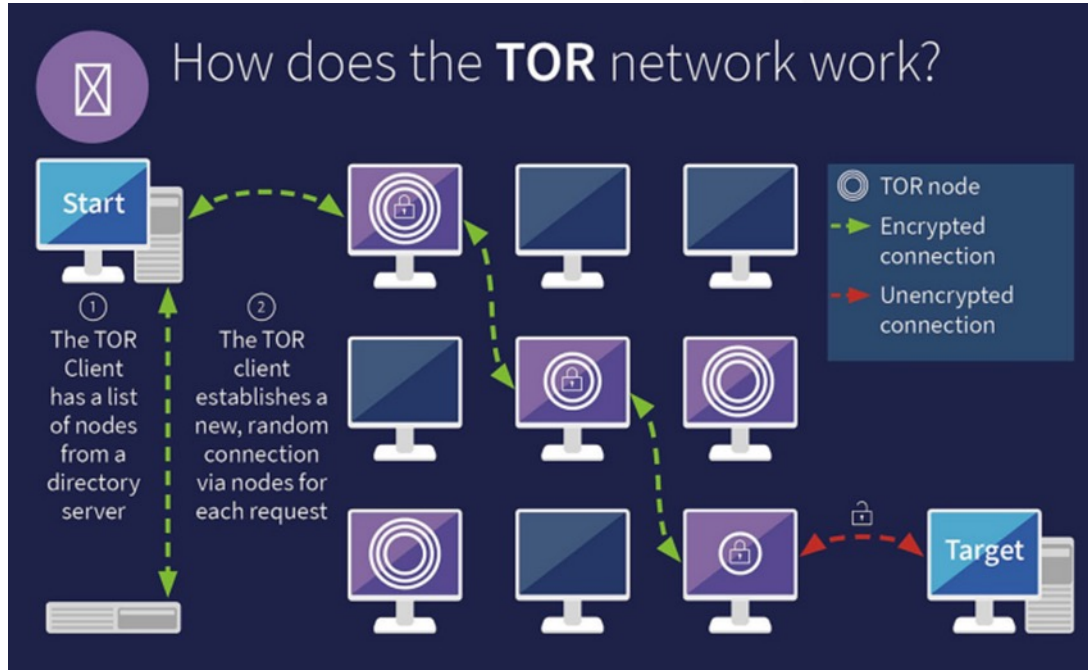
ACCESS DARKWEB



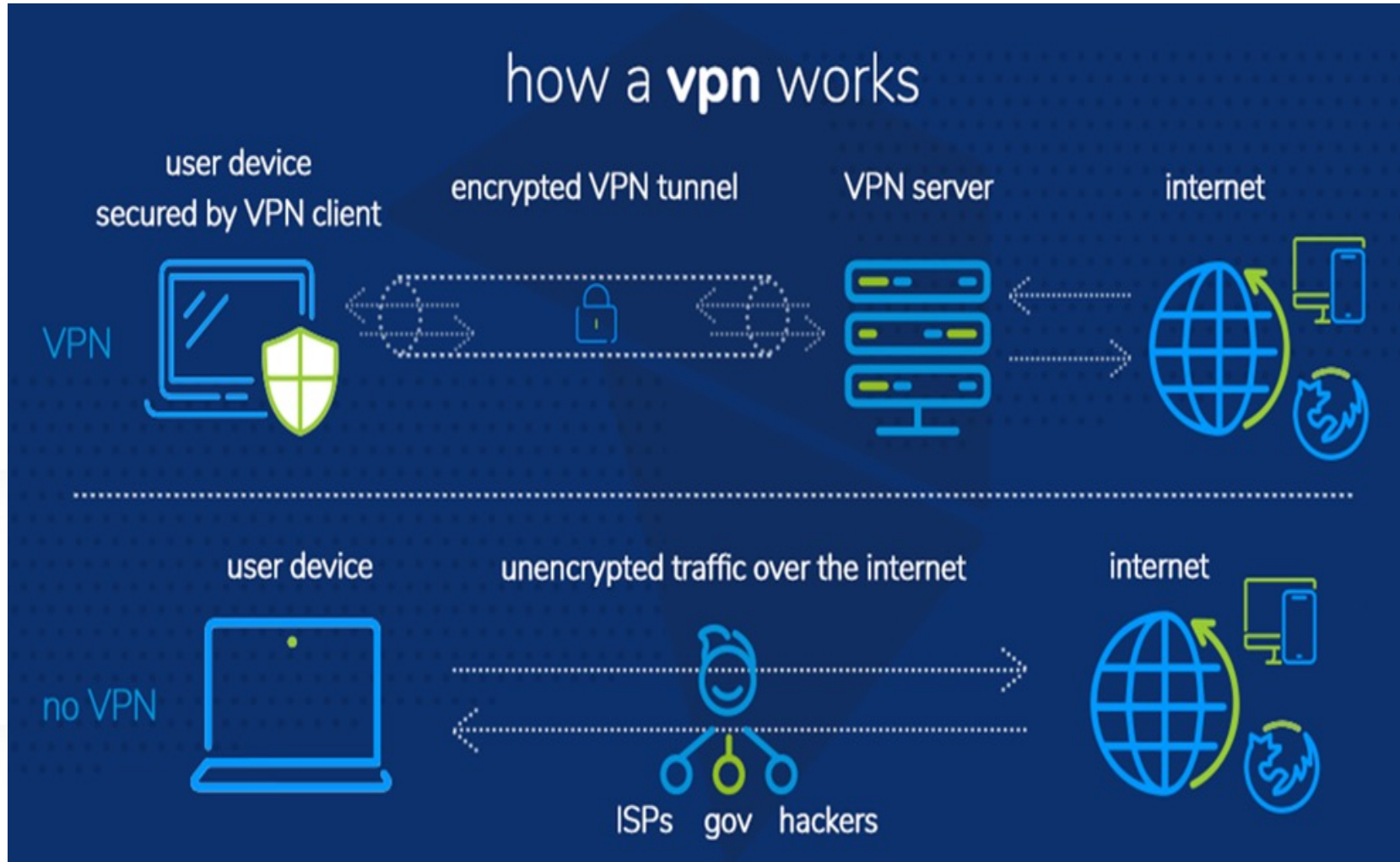
WHERE IS THE RISK



Tor Network

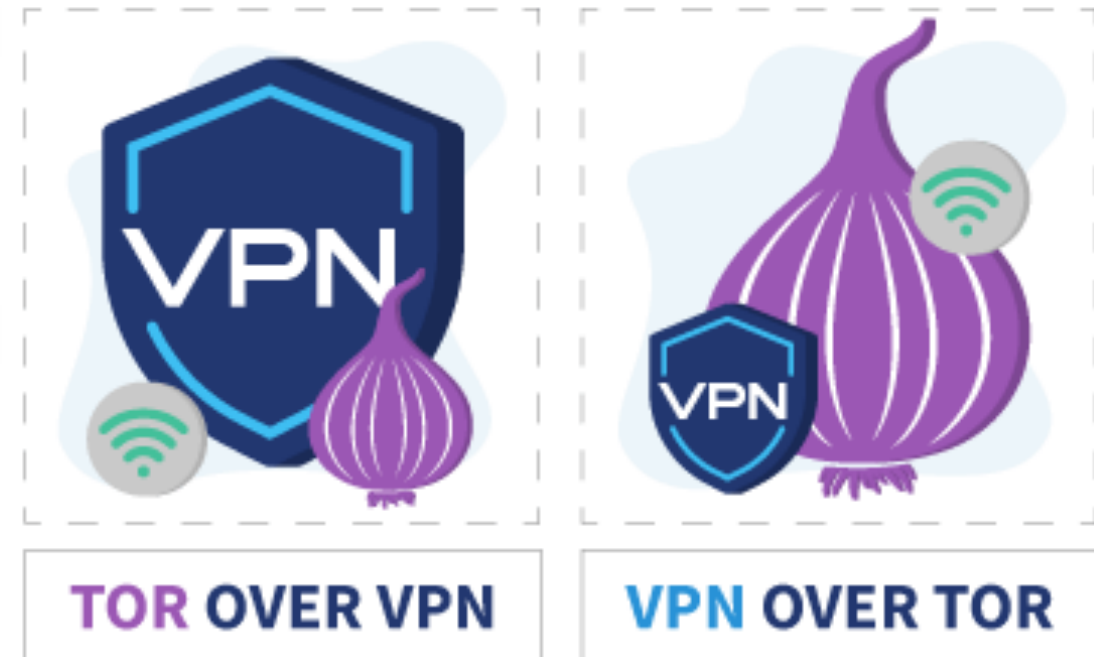


Tor Network



BEING ANONYMOUS

- ✓ Tails os
- ✓ Tor Browser
- ✓ Hotspot WiFi
- ✓ VPN
- ✓ Proxy
- ✓ OpenPGP
- ✓ Bitcoin
- ✓ Non-Personal Laptop
- ✓ Never shared information



DARKWEB TOUR



DARKWEB URL

SOCIAL MEDIA

- Reddit - <https://www.reddittorjg6rue252oqsxryoxengawnmo46qy4kyii5wtqnwfj4ooad.onion>
- Facebook - <https://www.facebookwkhpilnemxj7asaniu7vnjjbiltxjqhgye3mhbshg7kx5tfyd.onion>

EMAIL

- Mail2Tor - <http://mail2torjgmxgexntbrmhvgluavhj7ouul5yar6ylbvjkxwqf6ixkwyd.onion>
- Onion Mail - <http://pflujznptk5lmuf6xwadfgy6nffykdvahfbljh7liljailjbxrgvhfid.onion>

NEWS

- Tor Times - <http://tortimeswqlzti2aqbjoieisne4ubyuoeeiugel2layyudcfrwln76qd.onion>

SEARCH ENGINE

- Haystak - <http://haystak5njsmn2hqkewecpaxetahtwhsbsa64jom2k22z5afxhnpxfid.onion>

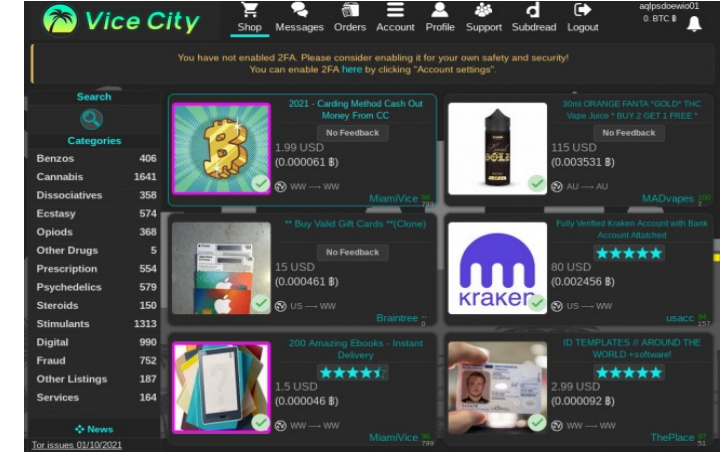
USE AT YOUR OWN RISK

UNDERGROUND FORUM/MARKET



BF





COMMUNICATION IN DARKWEB



TOX



Telegram

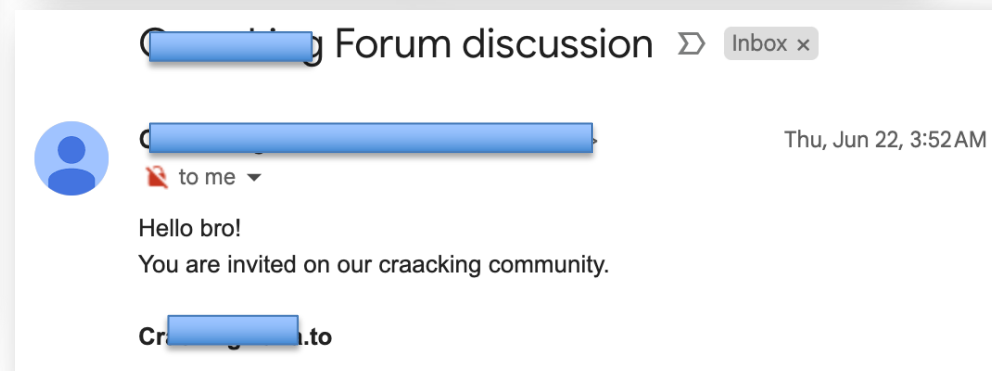
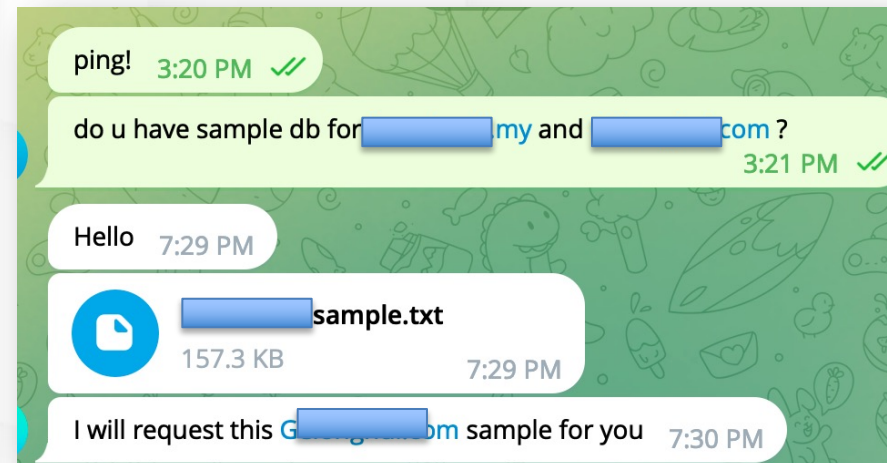
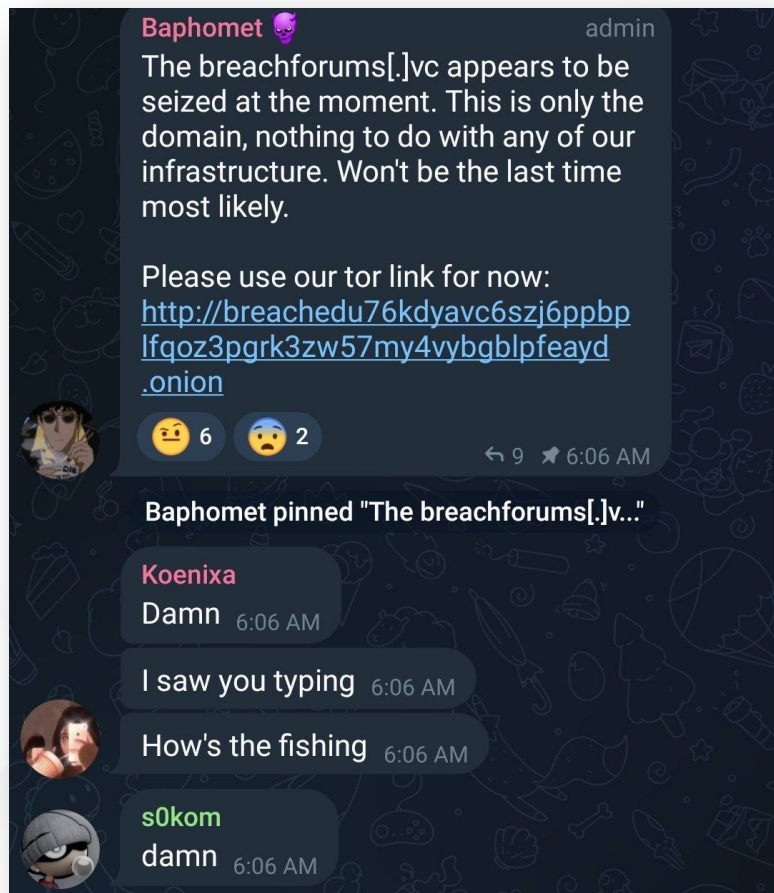


Discord



Proton Mail

COMMUNICATION IN DARKWEB



UNDERGROUND FORUM/MARKET

THIS DOMAIN HAS BEEN SEIZED

The domain for
RAID FORUMS

has been seized by the Federal Bureau of Investigation, the United States Secret Service, and the Department of Justice in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981, 982, inter alia, by the United States District Court for the Eastern District of Virginia as part of law enforcement action taken in parallel with Europol's Joint Cybercrime Action Task Force, the United Kingdom's National Crime Agency, the Swedish Police Authority, the Romanian National Police, the Internal Revenue Service Criminal Investigation and other international law enforcement partners.

THIS DOMAIN HAS BEEN SEIZED

The domains related to BreachForums
BF

have been seized by the Federal Bureau of Investigation, U.S. Department of Health and Human Services, Office of Inspector General, and the Department of Justice in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981, 982, inter alia, by the United States District Court for the Eastern District of Virginia as part of law enforcement action taken in parallel with the U.S. Secret Service, Homeland Security Investigations, the New York Police Department, the U.S. Postal Inspection Service, the Dutch National Police, the Australian Federal Police, the United Kingdom National Crime Agency, and Police Scotland.

THIS WEBSITE HAS BEEN SEIZED

OPERATION COOKIE MONSTER

Genesis Market's domains have been seized by the FBI pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Wisconsin. These seizures were possible because of international law enforcement and private sector coordination involving the partners listed below.

Been active on Genesis Market? In contact with Genesis Market administrators? Email us, we're interested: FBIMW-Genesis@fbi.gov

THIS HIDDEN SITE HAS BEEN SEIZED

Hive

The Federal Bureau of Investigation seized this site as part of a coordinated law enforcement action taken against Hive Ransomware.

This action has been taken in coordination with the United States Attorney's Office for the Middle District of Florida and the Computer Crime and Intellectual Property Section of the Department of Justice with substantial assistance from Europol

CASE STUDY – SITE OVERVIEW (FORUM)

Threads in
Subforum

Date + Time

[SELLING] Malaysia ABX Express Hacked Database - 36 Million Records (1 2) desorden	Regular Sales	14	1,640	06-04-2023, 11:23 AM Last Post: desorden
[SELLING] Corporate Databases of MNC Ben Line Agencies For Sale desorden	Regular Sales	8	698	06-04-2023, 11:18 AM Last Post: desorden
AirAsia Group (MY, ID, TH) Data Sample Leaked by DAIXIN Team hacxx	Compromised	0	46	05-10-2023, 01:30 AM Last Post: hacxx
✪ICHISTORE.CC✪ ALL IN ONE ACCOUNTS STORE ✪ EVERYTHING YOU NEED IS HERE!!! wizar0400	Regular Sales	1	537	05-01-2023, 03:46 PM Last Post: wizar0400
Hacxx IPTV Malaysia - Get Access to 37 Publicly Available Malaysian Channels hacxx	Hacking Tools	1	1,408	04-27-2023, 10:33 AM Last Post: hacxx
500 + PSD TEMPLATES Tools PRIVATE COLLECTION (1 2 3 4 5) Aged_Butler	Regular Sales	45	8,284	04-03-2023, 11:52 PM Last Post: mipiv88594
[SELLING] GOV EMAIL ACCESS TO THESE COUNTRIES (gov.Fr, gov.In, gov.Ng, gov.My, gov.Vn (1 2 3 4 5) Twofactors	Regular Sales	44	4,519	03-27-2023, 08:36 AM Last Post: Twofactors

Post Content

User Information
(Joined date, # of posts, etc.)

desorden
Registered (Bronze)
☆☆☆

Posts: 158
Threads: 31
Reputation: 0
Referrals: 0

Awards

Contact
Add to Buddy List
Add to Ignore List
Report User

desorden's Forum Info

Joined: 11-08-2021
Date of Birth: Hidden
Local Time: 06-22-2023 at 03:06 PM
Status: Offline

Stats

Last Visit: 06-04-2023, 04:53 PM

Total Posts: 158 (0.27 posts per day | 0.01 percent of total posts)
(Find All Posts)

Total Threads: 31 (0.05 threads per day | 0.02 percent of total threads)
(Find All Threads)

Time Spent Online: 8 Hours, 52 Minutes, 35 Seconds

Total Likes Received: 2 (0 per day | 0 percent of total 79290)
(Find All Threads Liked For — Find All Posts Liked For)

Total Likes Given: 0 (0 per day | 0 percent of total 79266)
(Find All Liked Threads — Find All Liked Posts)

Reputation: 0 (Details) (Rate)

Currency: 76 NSP (Donate)

Betting: (Bet Against This User)

Items: This user has no items. (View All Items)

Awards: 0 (Details)

Referrals (0): None

39

CASE STUDY – SITE OVERVIEW (MARKET)

Other 654
Security 388
Software 1061

Digital Goods 43611
Drugs 46109
Drugs Paraphernalia 278
Services 3835
Other 3370

Exchange

BTC	1.0
mBTC	1000.0
USD	16088.0
EUR	13729.3
GBP	12040.6
CAD	20552.8
AUD	20758.8
SEK	134094.9
NOK	130044.7
DKK	102160.3
TRY	61054.5
CNH	105455.4
HKD	124855.0
RUB	931264.5
INR	1030953.6
JPY	1822398.0

Onion mirrors

t3e6ly3uoif4zcw2.onion
verified

jd6yhuwcivehvdtdt4.onion
t3e6ly3uoif4zcw2.onion
7ep7ackunzdcw3l.onion
vilpaqbmrvizecjo.onion
igyifrhmvxq33sy5.onion
6qloctg6zq2kyacl.onion
x3x2dwb7jasax6tq.onion
bkjcpa2klkkmowwq.onion
xytjgcfcndzeby22.onion
nhib6cwhfsoyjugv.onion
k3pd243s57ftnpa.onion

19 20 ... 44 45 46 47 48 49 50 51 52 53 54 →

Hacking For Newbies

0.0000621
HappyEyes (5200) (4.79★)
WW → WW

ESCROW Order

731986-Hacker's Desk Reference

0.0001864
color (8000) (4.76★)
GB → WW

ESCROW Order

Premium Carding Package

0.0003107
OnePiece (7400) (4.83★)
PH → WW

ESCROW Order

6 BITCOIN RANSOMWARE EASY MONEY SYSTEM

0.0003107
TheWealthMaker (1550) (4.78★)
WW → WW

ESCROW Order

Go to Windows updates anonymously

0.0000621
HappyEyes (5200) (4.79★)
WW → WW

ESCROW Order

HACK ANYONE USING THEIR IP ADDRESS

0.0002486
TopNotchMoneyMaker (4500) (4.74★)
WW → WW

ESCROW Order

PayPal - Scam Page (Phishing site) [Looks Great]

0.00031
MicroDroper (2350) (4.91★)
WW → WW

ESCROW Order

PASSWORD MANAGER KIT

0.0001224
ElCartel (1800) (4.86★)
WW → WW

ESCROW Order

PayPal - Scam Page (Phishing site) [Looks Great]

Vendor MicroDroper (2350) (4.91★) (a 67/1/3)

Price 0.00031 (\$4.99)

Ships to Worldwide, Worldwide

Ships from PM

Escrow Yes

Price

Product Description

Product description

You will get all files for build phishing PayPal site. Look perfect.

We are not include support to the product, so if you have 0% knowledge about site building and php - please do not make an order.

Shipping options

0.00 (\$0) You will get download link

Product Reviews

Quantity 1 Add to cart

Product ratings

53d ★★★★★ Enter your comments here

Figure 1. Snapshot of Dream Market and an Example of a Phishing Product for PayPal.

CASE STUDY – SITE OVERVIEW (CARDING)

Home Buy CC CC Orders Buy Dumps Dump orders Checker Tickets support online

Dumps

Bulk order

Search Functionality

Bank Identification Number

Credit Card Type

Expiration Date

Bank Name

Country	Dump type	Dump mark	Debit/Credit
All All USA	All All Visa Master	All All Gold Platinum	<input checked="" type="checkbox"/> DEBIT <input checked="" type="checkbox"/> CREDIT
Bins	Bank & State & City	Base and other	Additional
380282, 376282	Bank: All State: All City: All	All	<input type="checkbox"/> Expiring 09/15 <input type="checkbox"/> Track1 Select <input type="text" value="Exp. date (1312)"/> <input type="text" value="Last 4 Digits"/> code: <input checked="" type="checkbox"/> 101 <input checked="" type="checkbox"/> 201

Didn't find the bin you were looking for? Need more dumps of particular bin? Try our partner's shop - [Bulk Orders - Low Prices!](#)

Clear Search


Bin	Card	Debit/Credit	Mark	Expires	Track 1	Code	Country	Bank	Base	Price	Cart
374328	AMEX	DEBIT	PREPAID	05/20	Yes	122	United States, WA, KENT, 98030	AMERICAN EXPRESS COMPANY <small>Dump or cc of this particular bank (BIN) cannot be replaced or refunded.</small>	American Sanctions 18	21\$	
517805	MASTERCARD	CREDIT	PLATINUM	12/17	Yes	101	United States, N/A, , 0	CAPITAL ONE BANK (USA) N.A. <small>Dump or cc of this particular bank (BIN) cannot be replaced or refunded.</small>	Imperium Romanum 2	52\$	
557621	MASTERCARD	DEBIT	PLATINUM	10/15	Yes	101	United States, NC, BURLINGTON, 27215	SUNTRUST BANKS INC. <small>Dump or cc of this particular bank (BIN) cannot be replaced or refunded.</small>	American Sanctions 18	28\$	

Figure 3. An Example of a Carding Shop Featuring Stolen Credit Cards

CASE STUDY – CRYPTOCURRENCY

The Dark Web Price Index 2022 – based on data scanning dark web marketplaces, forums, and websites, revealed:

- Credit card details and associated information. Cost between \$17-\$120
- Online banking login information costs \$45
- Hacked Facebook account: \$45
- Cloned VISA with PIN: \$20
- Stolen PayPal account details, minimum \$1000 balances: \$20.



PRODUCT	Avg. dark web price
Credit card details, account balance up to 5000	\$120
Credit card details, account balance up to 1000	\$80
Stolen online banking logins, minimum 2000 on account	\$65
Israel hacked credit card details with CVV	\$25
Hacked (Global) credit card details with CVV	\$15
Spain hacked credit card details with CVV	\$25
Cloned American Express with PIN	\$25
Canada hacked credit card details with CVV	\$18
Australia hacked credit card details w/CVV	\$23
Cloned Mastercard with PIN	\$20
Cloned VISA with PIN	\$20
Stolen online banking logins, minimum 100 on account	\$35
Australia hacked credit card details with CVV	\$30
Walmart account with credit card attached	\$10
USA hacked credit card details with CVV	\$17
UK hacked credit card details with CV	\$20

SOURCE: PRIVACY Affairs

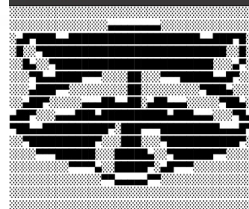
CASE STUDY – SAMPLE DATA

```

60K COMBOLIST Malaysia NEA
File Edit View
dascissors@live.com.my:yvonneltiva
kbak_gjin@yahoo.com.my:azzin
sy_wan75@yahoo.com.my:664809
haffiaddin80@yahoo.com.my:haddin
chikz_mokz@yahoo.com.my:coklat
mazmdisa@yahoo.com.my:8thatCuervo
antihipokrit_pink@hotmail.com.my:kentang1
ncrhorse@yahoo.com.my:oceanblue94qwe
cheryl_bella@yahoo.com.my:017andy@fm116@msn.com
annadha91@hotmail.com.my:annadha19
siti zahidah89@yahoo.com.my:yyda89
sayaaare@yahoo.com.my:Syahira93
aslimiri@yahoo.com.my:jm6580
zaphianrizalazmi@yahoo.com.my:750316zre
nakadnaz@yahoo.com.my:123123
puteri_nana96@yahoo.com.my:cincan
embam7063@yahoo.com.my:nunzak1
atoksss@yahoo.com.my:007007
utkdm1d@yahoo.com.my:helmy17
geronimo1_509@yahoo.com.my:geronimo1_509
anisaqaela@hotmail.com.my:sanis98
nonanis_giri@yahoo.com.my:reza224
mohdaniFsiddiq_sazali@yahoo.com.my:sazali2003
suraiyaalihamad@yahoo.com.my:5853klarrisa
nuar_ahmad@yahoo.com.my:030983
manjalara265@yahoo.com.my:loveLove12
andrewchia90@hotmail.com.my:52013145
budak_4n3@yahoo.com.my:cen311974
hcvisepul@yahoo.com.my:0139554324
paulinehnm6@yahoo.com.my:cf523906d49
Ln 60505, Col 38 100% Unix (LF) UTF-8

```

System Info.txt



User ID: f05fa7dd-2892-454a-8d13-0d76147be2e|amin_
Last seen: Tue Mar 21 2023 16:22:18 GMT+0100 (Central European Standard Time)
Build: 64181a...0382c2

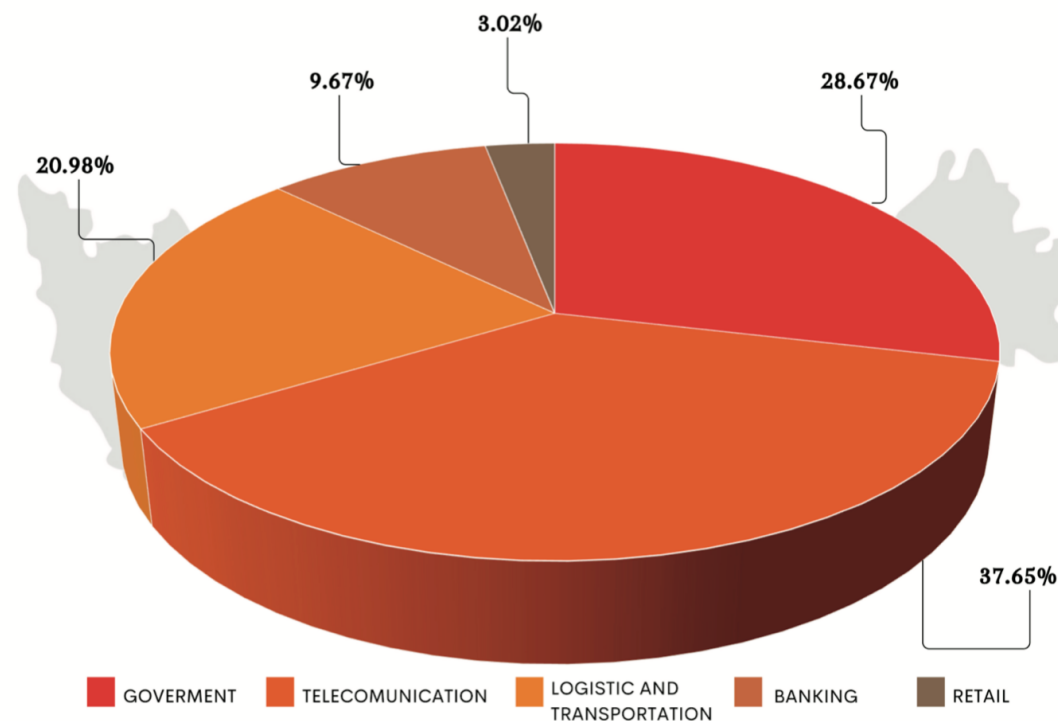
IP info: MY 124.13.41.180

System Information:

- Locale: English
- Time zone: +480 minutes from GMT
- OS: Windows 10 Pro
- Architecture: x64
- CPU: AMD Ryzen 5 2600 Six-Core Processor (12 cores)
- RAM: 16317 MB
- Display size: 1920x1080
- Display Devices:
 - 0) NVIDIA GeForce GTX 1080 Ti

Installed applications:

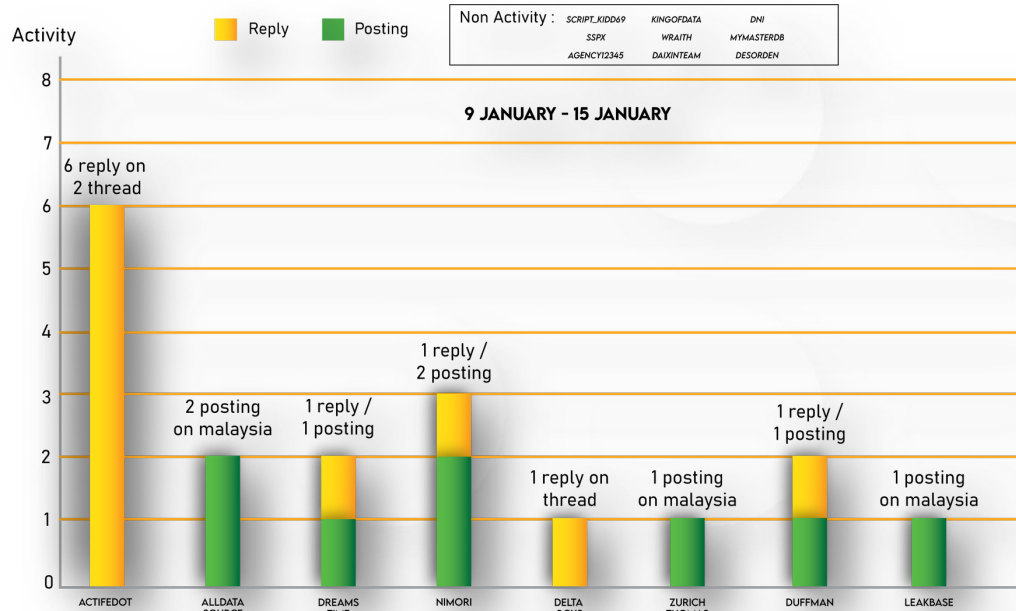
- 7-Zip 19.00 (x64)
- AMD Software 9.0.0.000.8
- Need for Speed™ Heat
- Even Truck Simulator 2



Total data leak in Q1 and Q2

Visualization Finding Threat Actor Monitoring

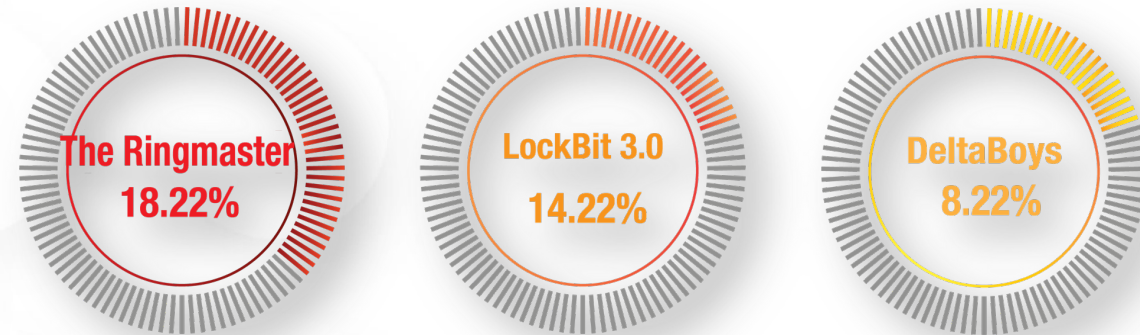
1. Threat Actor Activity monitored by weekly



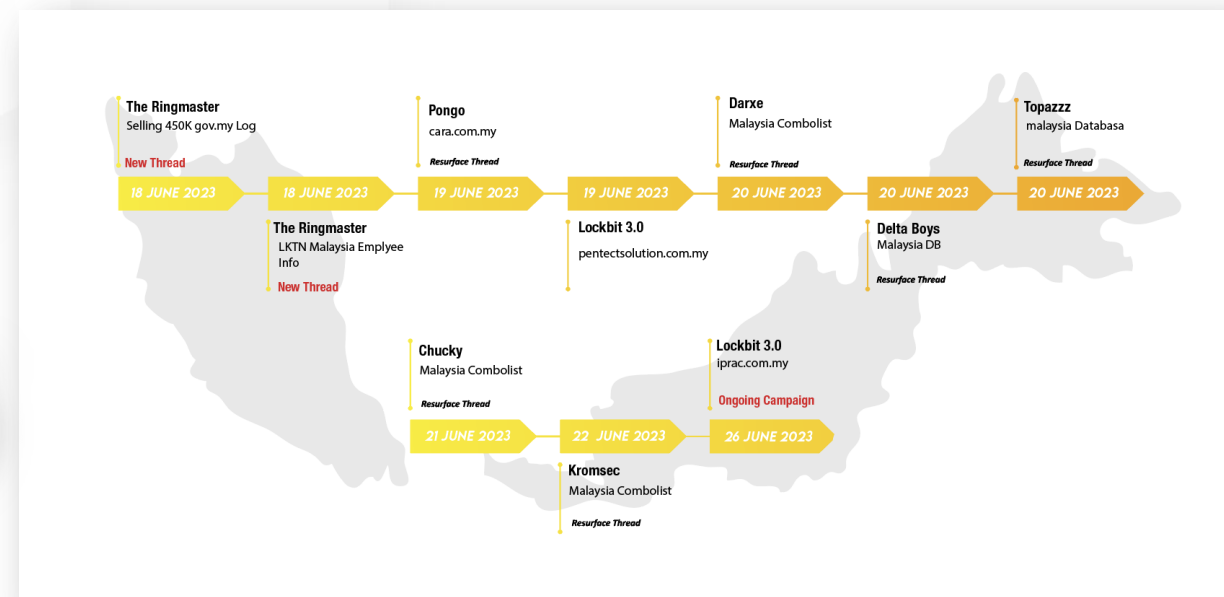
2. Total Threat Actor and Incident happened in Malaysia



3. Top 3 Active Threat Actor

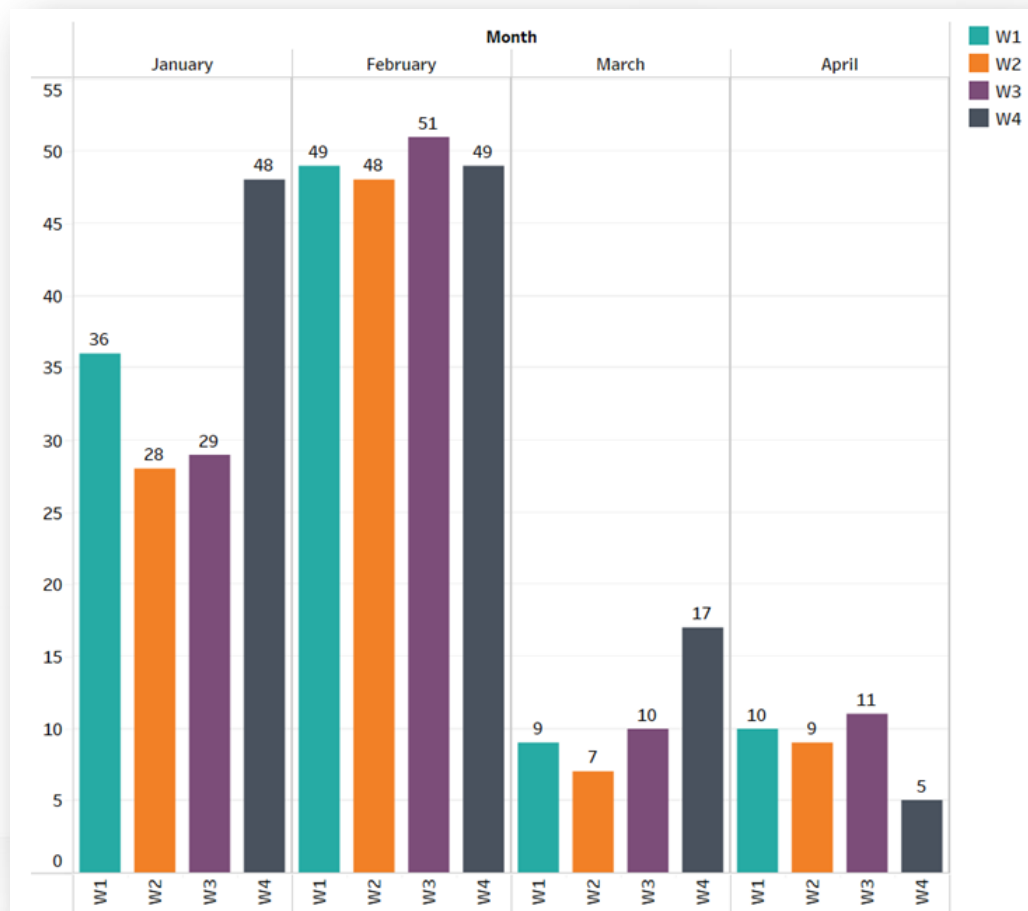


4. Timeline Threat Actor Activity by Weekly



Incident Landscape in Malaysia

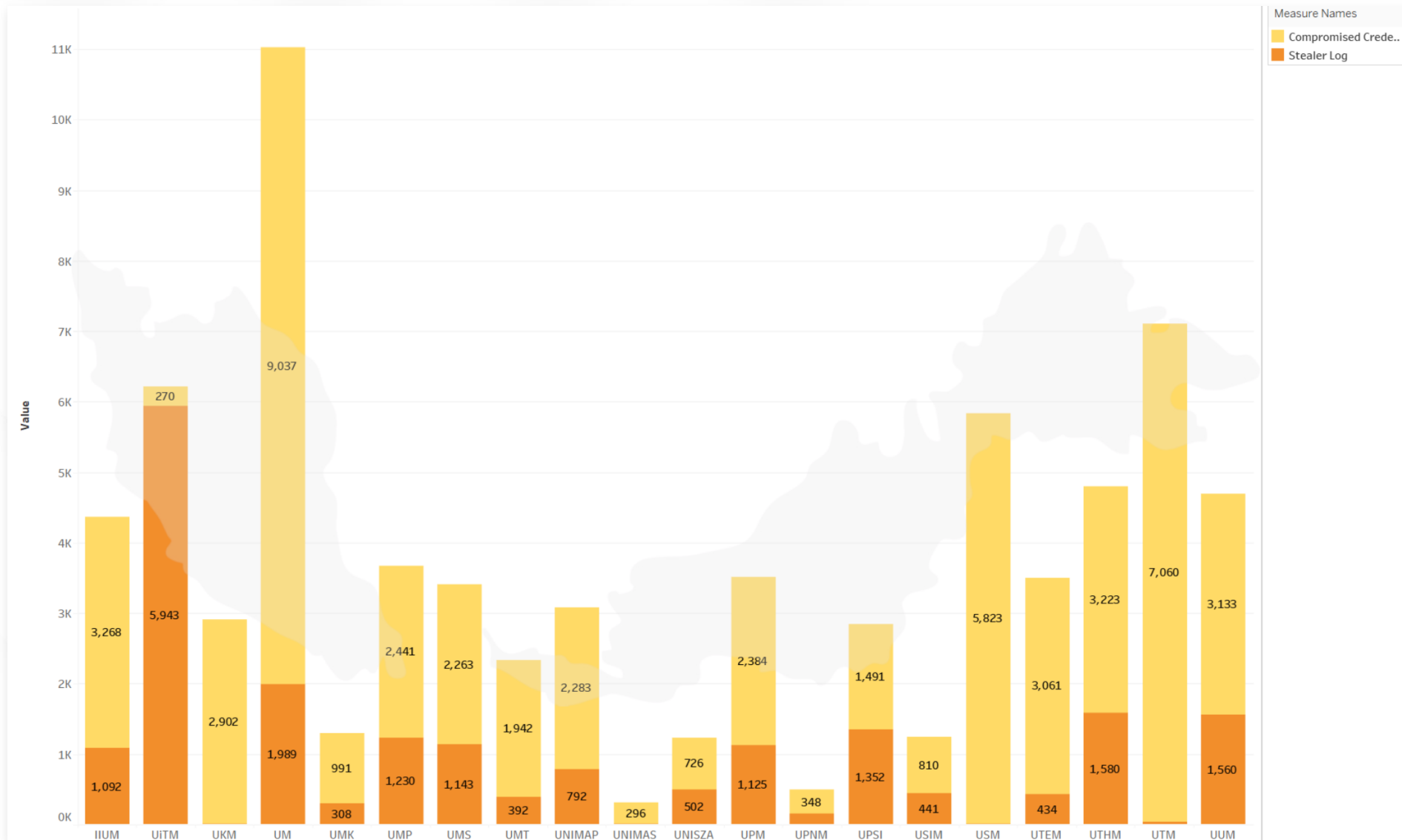
1. Graph trend for cyber incident happened in Malaysia.



2. Infographic for summarizing cyber incident monthly.

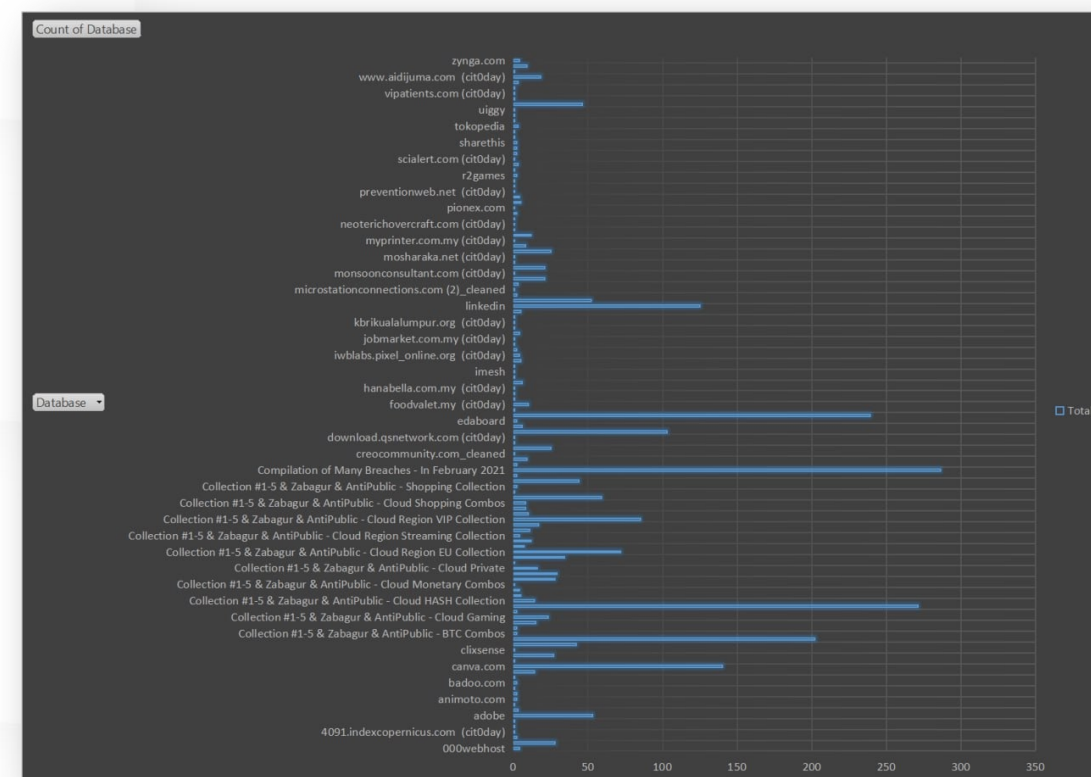


Dark Web Monitoring | IPTA

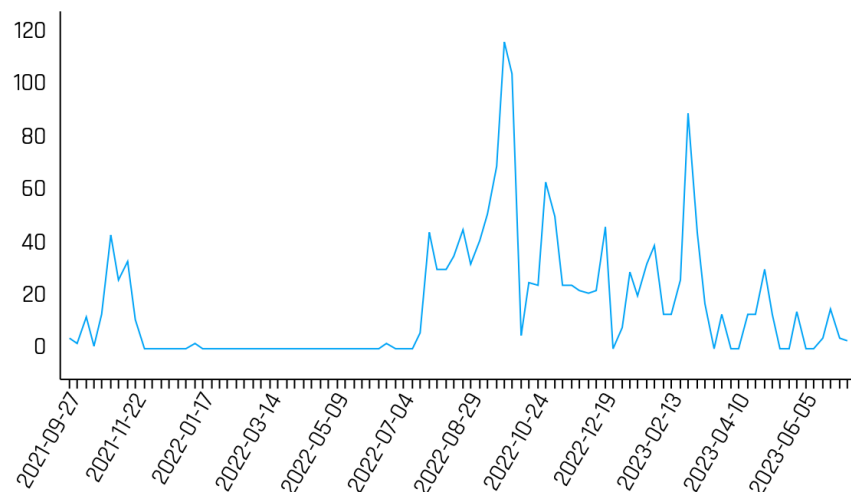


CASE STUDY – SAMPLE DATA (EDU.MY)

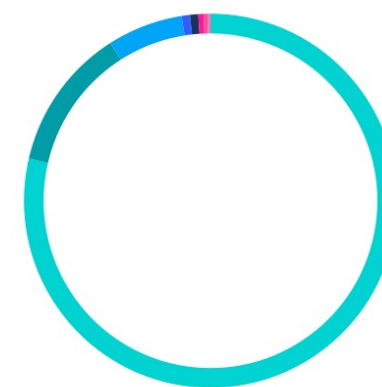
Date	Domain	Email	IP Address	Username	Password	Name	Vin
2023-	.edu.my	a				mad_Mohamed_7	
2023-	.edu.my	su					
2023-	.edu.my	m					
2023-	.edu.my	h					
2023-	.edu.my	fa					
2023-	.edu.my	fa			2602		
2023-	.edu.my	sh			ahna82		
2023-	.edu.my	co					
2023-	.edu.my	n					
2023-	.edu.my	ro					
2023-	.edu.my	h					
2023-	.edu.my	n					
2023-	.edu.my	n				family	
2023-	.edu.my	m					
2023-	.edu.my	fa			5		
2023-	.edu.my	fa					
2023-	.edu.my	ke					
2023-	.edu.my	e					
2023-	.edu.my	a					
2023-	.edu.my	fi					
2023-	.edu.my	a					
2023-	.edu.my	m					
2023-	.edu.my	fe					
2023-	.edu.my	a					
2023-	.edu.my	li					
2023-	.edu.my	ch					
2023-	.edu.my	h					
2023-	.edu.my	w					
2023-	.edu.my	zi					
2023-	.edu.my	kl					
2023-	.edu.my	a			5774		
2023-	.edu.my	ro				Rosshalila Sharip	
2023-	.edu.my	sa					



THREAT ACTOR PROFILING



TIMELINE FOR INDICATED TIMEFRAME



forum_breached	77%
forum_sinisterly	12%
forum_raidforum	6%
forum_breach	1%
forum_cracked	1%
forum_nulledbb	1%
forum_nulled	1%
telegram	1%

STATISTIC SITE THREAT ACTOR REGISTERED



Data_leak	22%
Download_link	12%
Bitcoin	11%
Cryptocurrency	11%
Hacking	10%
Email_address	10%
email	10%
Email_domain	6%
Drugs	4%
Fraud	4%

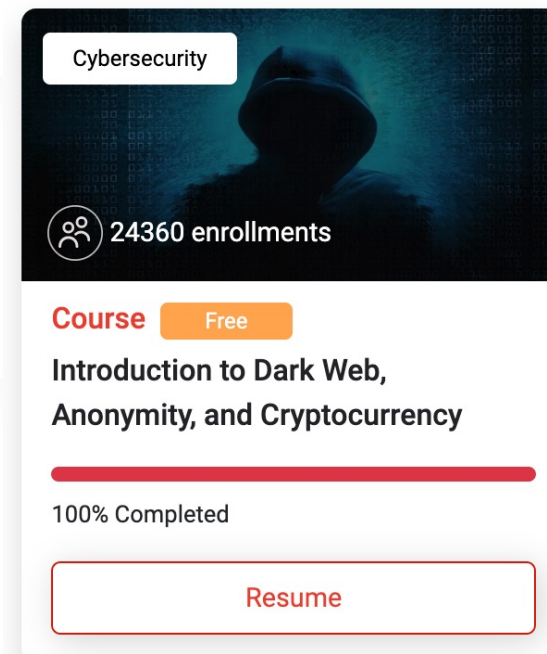
STATISTIC ACTICITIES OF THREAT ACTOR IN THE FORUM

THREAT ACTOR PROFILING



DARKWEB CERTIFICATE

Introduction to Dark Web, Anonymity, and Cryptocurrency



SOURCE: <https://codered.eccouncil.org/course/introduction-to-dark-web-anonymity-and-cryptocurrency>

THANK YOU

CyberSecurity Malaysia
Level 7, Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya
Selangor Darul Ehsan, Malaysia

T +603 8800 7999 | **F** +603 8008 7000 | **H** +61 300 88 2999

www.cybersecurity.my | info@cybersecurity.my

 CyberSecurityMalaysia

 cybersecuritymy

 cybersecuritymy

 CyberSecurity Malaysia

 cybersecurity_my

